U.S. Department of Transportation

Office of the Secretary of Transportation

ORDER

DOT 1600.26A

7-25-90

Subject: DEPARTMENT OF TRANSPORTATION PHYSICAL SECURITY PROGRAM

1. PURRPOSE. This Order defines organizational relationships in the Department of Transportation (DOT) physical security program; prescribes procedures for planning the physical security program; provides guidance on the conduct of physical security inspections and surveys for offices and facilities determined to be mission-essential or vulnerable to theft, robbery, burglary, and other forms of criminal activity; and prescribes reporting procedures for applicable reports to the Office of the Assistant Secretary for Administration.

2. CANCELLATION. DOT 1600.26, Department of Transportation Physical Security Manual, dated 11-29-77.

3. SCOPE. This Order applies to all Operating Administrations and Secretarial Offices of DOT having responsibility for the control, movement, storage, maintenance, and/or physical security of personnel, material, equipment, facilities, and documents.

4. REFERENCES.

a. Title 41, United States Code, Part 101, Management of Buildings and Grounds.

b. Executive Order 12356, National Security Information.

c. National Communications Security Instruction (NACSI) 4008, Safeguarding Communication Security (COMSEC) Facilities.

d. Delegation of Authority from the General Services Administration (GSA) for lease operation of buildings.

e. DOT 1100.60A, DOT Organization Manual, of 11-14-88, delegates authority to the Assistant Secretdry for Administration to formulate and recommend Departmental policies, plans, and programs for all aspects of security and further describes the mission of the Office of the Secretary (OST), Office of Security.

f. DOT 1600.23, Demonstrations in or Near-Government Buildings, of 3-3-72, promulgates the DOT national policy regarding demonstrations at Government buildings.

DISTRIBUTION: All Secretarial Offices
All Operating Administrations

OPI: Office of Security

g. DOT 1600.24, Perimeter Security Controls for the DOT Headquarters Buildings, of 8-21-72, establishes entry and exit security controls for the DOT headquarters building.

h. DOT 1600.25, Consolidation of Physical Security Services for the DOT Washington Headquarters Facilities, of 4-27-72, establishes a consolidated physical security program for DOT headquarters facilities under the Director, Office of Security, OST, (M-70).

i. DOT 1660.1A, Removal of Equipment from Department of Transportation Buildings, of 10-21-74, establishes controls over the removal of equipment from DOT-occupied premises during and after normal duty hours.

j. DOT 1660.4, Physical Security Review of New Facilities, Office Space or Operating Areas, of 6-13-75, prescribes DOT requirements for reviewing the physical security environment when obtaining new facilities, office space, or operating areas for use by any DOT element.

k. DOT 1660.5, Locking System for the Department of Transportation Headquarters (Nassif) Building, of 2-15-80, describes the corridor door locking system in the Nassif Building and assigns responsibilities for carrying out the various aspects of the system.

l. United States Coast Guard (USCG), Physical Security Manual (COMDTINST - M5530.1).

5. BACKGROUND. Physical security controls are an essential element in the protection of Departmental offices, facilities, personnel, and resources. To be effective, such controls must be integrated and complement each other. Using the guidance contained in this Order, office and facility managers should, in concert with the servicing security element (see Appendix C for servicing security element/cognizant security officer for each-mode) take a systems approach in the analysis of the physical protection requirements for the particular office or facility. It is also important to recognize the limitations of the physical security controls; namely, that they only serve to deter and delay and cannot be expected to preclude a determined intruder from penetrating an office or facility for illicit purposes. Management must include security from the concept stage.

6. **EXPLANATION OF TERMS.**

a. Physical Security. That part of security concerned with physical security measures and designed to safeguard personnel; to prevent unauthorized access to equipment, facilities, material, and documents; and to safeguard them against espionage, sabotage, damage, and theft,'

b. Physical Security Program. The interrelationship of various mutually supporting and interrelated security disciplines used to produce a comprehensive approach to physical security matters. These components include, but are not limited to, a physical security plan, physical security inspections and surveys, and a continuing assessment of threat versus an activity's physical security posture.

c. Physical Security Plan. A comprehensive written plan assuring proper and cost effective use of resources to prevent or minimize loss or damage from theft, espionage, sabotage, and other criminal or disruptive activities.

d. Physical Security Inspection. A formal, recorded assessment of a physical security plan and/or program at a specific facility or office. The inspector will check for compliance with the physical security plan. The assessment will contain conclusions and recommendations that are the result of an exacting on-site examination of barriers, guard/security forces, communications, transportation, contingency/emergency support, protective lighting, intrusion detection systems, and other physical security measures used to protect offices and facilities from loss, theft, destruction, sabotage, or compromise. This includes crime prevention measures for mission-essential or vulnerable areas (see paragraph 12 for details).

e. Physical Security Survey. The physical security survey is an exacting on-site examination of barriers, guard/security forces, communications, transportation, contingency/emergency systems, and other physical security measures. It is the basis for the development of an efficient and effective physical security plan (see paragraph 13 for details).

f. Mission-Essential/Vulnerable Areas. Certain facilities and operations within an organization or installation which, by virtue of their function, are essential to successful accomplishment of the organization's mission and functions. This also includes areas which may be nonessential to the organization'soperational mission and functions, but may be vulnerable to theft, trespass, damage, or other criminal activity (see Appendix B).

7. POLICY. It is the policy of the DOT that the Operating Administrations and Secretarial Offices establish a physical security program that complies with this Order and applicable national policies and standards. This program will assure that adequate physical security is provided for the Department's facilities, offices, mission-essential, and vulnerable areas to include the formulation of physical security plans. It will also provide for periodic physical security inspections and surveys.

8. RESPONSIBILITIES.

a. The Assistant Secretary for Administration has Departmental responsibility for programs, policies, and procedures relating to physical security and will provide Departmentwide guidance and assistance in these matters.

b. The Director, Office of Security, OST, is the executive agent of the Assistant Secretary for Administration for the physical security program and also is responsible for:

(1) Ascertaining the need for formulating and recommending Departmental physical security policies, plans, and programs.

(2) Operating the physical security program for the OST.

(3) Designating cognizant security offices for the Operating Administrations, offices, and facilities (see Appendix C).

(4) Reviewing and approving physical security orders that are drafted to implement this Departmental Order.

(5) Assuring that all counterintelligence aspects of physical security plans and programs, specifically those related to protecting the DOT from espionage, sabotage, and subversion are carefully monitored.

(6) Assuring (in coordination with other program offices as appropriate) compliance with national policies and standards for the physical security of cryptographic facilities, automatic data processing facilities, communications facilities, and sensitive research and development facilities.

(7) Coordinating the provision of threat data and its analysis in support of facility and/or office physical security plans.

(8) Conducting physical security inspections to assure compliance with the Department's physical security program.

c. The Administrator, Federal Aviation Administration (FAA), and the Commandant, United States Coast Guard (USCG), are responsible for the following:

(1) Establishing and maintaining. a physical security program that complies with the Department's policy (paragraph 7) and applicable national policies and orders. FAA and USCG orders which establish physical security programs will be reviewed and approved by the Office of Security, OST, and will be viewed as complying with the requirement for a security plan.

(2) Assuring the completion of periodic physical security surveys and inspections of mission-essential and vulnerable facilities and offices under their control.

(3) Assuring that plans, project drawings and specifications for initial construction and/or modification are submitted to the cognizant security office for review and approval prior to issuing of the contract.

(4) Providing statistics to the Office of Security, OST, on a fiscal year basis, discrepancies of the previous year inspections. Such statistics are to provide indicators of program effectiveness. The Office of Security, OST, will identify such specific reporting requirements at least 90 days prior to the beginning of the fiscal year to be reported.

d. Operating Administrators (excluding FAA and USCG), and Assistant Secretaries, in coordination with the Office of Security, OST, are responsible for the following:

(1) Establishing and maintaining a physical security program that complies with this Order and applicable national policies and orders. Orders which establish the physical security program will be reviewed and approved by the Office of Security, OST.

(2) Identifying systems, material, equipment, offices, facilities, personnel, and functional activities for which they have Departmental responsibility that require physical security.

(3) Developing security criteria for consideration in initial plans for all new or modified construction projects. Coordinating construction of computer rooms with the Computer Security Officer. .

e. All Office Directors, Regional Administrators, Regional Directors and Field Office Directors (excluding FAA and USCG) are responsible for assuring that precautions are taken to safeguard personnel and property under their supervision. They will implement a formal physical security program' and establish a physical security plan (refer to paragraph 11 of this Order) that complies with. stated program policies and procedures. They will designate security representatives or coordinators to plan, formulate, and coordinate physical security matters (see DOT 1600.25).

f. Security representatives or coordinators (excluding FAA and USCG) are responsible to their Office Directors, Regional Administrators, Regional Directors, and Field Office Directors for: .

(1) All facets of the physical security program; and

(2) Reviewing (in coordination with the cognizant security office) all plans for new or modified construction to assure that all possible physical safeguards are considered in the design phase, physical security deficiencies are eliminated or minimized, and that construction complies with sound physical security principles.

g. Cognizant security offices (see Appendix C) (excluding FAA and USCG) are responsible for the following:

(1) Conducting or assuring that initial and periodic physical security inspections and surveys are conducted; and

(2) Coordinating with Office Directors, Regional Administrators, Regional Directors, and Field Office Directors regarding the formulation of physical security plans.

9. EXEMPTIONS.

a. Local host/tenant agreements may exempt certain tenant activities because they are subject to physical security regulations of their own departments or agencies. The concerned security officer or security representative should coordinate with the supervisor of each such tenant facility or office to determine whether they are exempt from this Order.

b. The cognizant security office may exempt from physical security inspection requirements, facilities determined not to be mission-essential and which retain a negligible amount of cash and pilferable items on the premises.

10. REPORT CLASSIFICATION. Reports of physical security surveys/inspections will be classified when appropriate. The report will be classified in accordance with DOT 1640.4C, Classification, Declassification, and Control of National Security Information, of 11-22-83. When the report contains privileged or proprietary information, it will be marked "'For Official Use Only" in accordance with DOT 1640.1, Control and Protection of "For Official Use Only" Information, of 12-27-71.

11. PHYSICAL SECURITY PLANNING. This section serves as guidance and instruction to the Operating Administrations (excluding FAA and USCG) and Secretarial Offices with regard to the formulation of a physical security plan.

a. Planning Considerations.

(1) In order to achieve adequate protection for a facility or office, managers or directors will develop detailed written plans which will utilize available resources in the most cost-effective manner.

g. Cognizant security offices (see Appendix C) (excluding FAA and USCG) are responsible for the following:

(1) Conducting or assuring that initial and periodic physical security inspections and surveys are conducted; and

(2) Coordinating with Office Directors, Regional Administrators, Regional Directors, and Field Office Directors regarding the formulation of physical security plans.

9. EXEMPTIONS.

a. Local host/tenant agreements may exempt certain tenant activities because they are subject to physical security regulations of their own departments or agencies. The concerned security officer or security representative should coordinate with the supervisor of each such tenant facility or office to determine whether they are exempt from this Order.

b. The cognizant security office may exempt from physical security inspection requirements, facilities determined not to be mission-essential and which retain a negligible amount of cash and pilferable items on the premises.

10. REPORT CLASSIFICATION. Reports of physical security surveys/inspections will be classified when appropriate. The report will be classified in accordance with DOT 1640.4C, Classification, Declassification, and Control of National Security Information, of 11-22-83. When the report contains privileged or proprietary information, it will be marked "'For Official Use Only" in accordance with DOT 1640.1, Control and Protection of "For Official Use Only" Information, of 12-27-71.

11. PHYSICAL SECURITY PLANNING. This section serves as guidance and instruction to the Operating Administrations (excluding FAA and USCG) and Secretarial Offices with regard to the formulation of a physical security plan.

a. Planning Considerations.

(1) In order to achieve adequate protection for a facility or office, managers or directors will develop detailed written plans which will utilize available resources in the most cost-effective manner.

(3) Physical security planning is a continuing process. Changes in operations and activities within an organization or facility also require that adjustments be made in the security plans.

(4) All planned security measures must be employed so that they complement and supplement each other.

(5) Physical security plans must be tailored to the security needs and location of each operation, facility, and installation. A basic element of each security plan is a security force capable of assuring enforcement of established security measures and procedures. Other measures, such as barriers, protective lighting, communications, closed circuit television surveillance, automated entry control systems, and other means will be incorporated into security plans, as, applicable, to increase the effectiveness of the security force. Physical security elements are best organized in-depth to minimize or eliminate any security weakness. The selection and utilization of security measures is the responsibility of security planners and facility managers working in close coordination.

(6) The security plan will contain specific guidance on planning and action to be taken in response to demands, threats, or actions by terrorist groups. Facility and office managers will not submit to blackmail threats by such groups -and will not pay nor plan for payment of ransom. DOT officials having supervision of Government-owned, contractor-operated activities will develop plans which provide appropriate response to ransom threats or demands. Such officials will develop appropriate contingency plans if the contractor, having been fully apprised of U.S. Government policy concerning ransom payment, indicates an intent to yield to such threats rather than accept the risk.

(7) Physical security plans will provide definitive procedures for liaison between facility or office security forces, the GSA, Federal Protective Service, fire departments, explosive ordinance disposal teams, and local police, as appropriate. Jurisdictional authority of the security force (exclusive, concurrent, or proprietary) and their operational relationships with outside police agencies will be clearly established.

b. Security Plan Format. The security plan format will provide proper and economical utilization of personnel while providing flexibility to meet emergencies. A sample security plan is included at Appendix A.

c. Standards of Security. Security standards contained in appropriate security orders in the 1600 series should be used as guides in planning a physical security program. In the planning process, consideration should be given to the following-:

(1) Indicators that might reflect deficiencies affecting a facility or office include:

(a) Evidence that any part of the facility or office is being used for other than lawful or authorized practices.

(b) Indication that perimeter security is less than adequate-.

(c) Indication that fences, other barriers, and/or lights are needed.

(d) Disclosure that control and identification of persons entering and leaving a facility or installation are inadequate.

(e) Indication that secure communications, personnel, equipment, plans, and procedures to support facility or office physical security are inadequate, not exercised or tested periodically, or slow in response.

(7) Physical security plans will provide definitive procedures for liaison between facility or office security force?, the GSA, Federal Protective Service, fire departments, explosive ordinance disposal teams, and local police, as appropriate. Jurisdictional authority of the security force (exclusive, concurrent, or proprietary) and their operational relationships with outside police agencies will be clearly established.

b. Security Plan Format. The security plan format will provide proper and economical utilization of personnel while providing flexibility to meet emergencies. A sample security plan is included at Appendix A.

c. Standards of Security. Security standards contained in appropriate security orders in the 1600 series should be used as guides in planning a physical security program. In the planning process, consideration should be given to the following:

(1) Indicators that might reflect deficiencies affecting a facility or office include:

(a) Evidence that any part of the facility or office is being used for other than lawful or authorized practices.

(b) Indication that perimeter security is less than adequate.

(c) Indication that fences, other barriers, and/or lights are needed.

(d) Disclosure that control and identification of persons entering and leaving a facility or installation are inadequate.

(e) Indication that secure communications, personnel, equipment, plans, and procedures to support facility or office physical security are inadequate, not exercised or tested periodically, or slow in response.

12. PHYSICAL SECURITY INSPECTIONS.

a. Relationship to Physical Security Surveys. Physical security inspections of mission-essential or vulnerable facilities and offices are necessary adjuncts to the security survey, but in no way replace the requirements for such surveys. Physical security inspections are conducted to assure compliance with the physical security plan and the physical security program.

b. Inspection Scheduling. Office or facility mission-essential or vulnerable areas will be scheduled by the cognizant security office. Physical security inspections will be conducted on a periodic basis. Physical security inspections will not be conducted during the preparatory steps and the on-site examination stage of the physical security survey. Inspections should be made when there is any change in the activity/installation that may impact on existing physical security or when there are any indications or reported incidents of significant or recurring criminal activity, or every five years.

c. Mission-Essential/Vulnerable Areas to be Inspected. Appendix B shows examples of activities which may be considered mission-essential/vulnerable areas and which are particularly suitable for physical security inspections.

d. Inspection Procedures.

(1) Inspection personnel from the cognizant security office will conduct entrance and exit interviews with the facility or office manager or his/her designated representative. Findings of the inspection will be discussed at the exit interview, and a copy of the inspection report will be forwarded through appropriate channels to the facility or office manager within 30 days following completion of the inspection.

(2) Inspections will be conducted during duty and nonduty hours and during daylight and hours of darkness to properly assess total facility/ installation operations.

(3) Physical security inspectors will be granted access to DOT facilities, records, and information based on a need to know and consistent with the inspector's security clearance and the provisions of applicable orders and instructions.

e. Correction of Deficiencies Through Submission of Work Orders.

(1) Deficiencies noted on physical security inspection reports may be used by facility managers, budget officers, and other service agencies for programming funds, requesting construction, and communications work.

(2) Work-order requests and submission of construction and communications requirements will not be considered a correction of noted deficiencies. Pending completion of corrective action, compensatory measures within available resources will be placed in effect. Periodic liaison by the concerned security representative or facility/office manager and the appropriate service agency responsible for completion of work will be maintained to assure expeditious correction of deficiencies.

(3) uncorrected deficiencies for which work orders were submitted will be reported as deficiencies on subsequent physical security inspection reports until work is completed and all corrections have been made. Physical security inspectors will verify that work orders and other requirements were actually submitted to the appropriate service agency, that corrective action is in progress, and that adequate interim compensatory measures are actually in effect.

13. PHYSICAL SECURITY SURVEYS.

a. Relationship to Physical Security Plan. The physical security survey is an exacting on-site examination of barriers, guard/security forces, communications, transportation, contingency and emergency systems, and other physical security measures. The initial survey will serve as the basis for a physical security plan. The physical security plan is a key part of the local

physical security program. It must be closely reviewed to properly evaluate the effectiveness of security personnel, perimeter barriers, protective lighting, security communications, entry control and surveillance systems, visitor control, and other security considerations necessary to protect personnel and Government property.

b. Physical Security Survey Scheduling. When it is feasible, a physical security survey is conducted on the activation of a facility or office and when significant changes occur to facilities or operations which invalidate previous survey data. It will be scheduled and conducted by the cognizant security office. An initial survey is the first complete physical security evaluation of a specific site or operation. It will be conducted when a facility's or office's mission-essential or vulnerable areas are activated or when no record exists of a prior physical security survey.

c. Assessment of Physical Security Survey. Following conduct of the survey, the cognizant security office will make an assessment of the survey report, the facility's or office's mission and functions, and potential security threat. This assessment will be the basis for Facility and Office Directors and Managers to:

(1) Develop an action list which indicates a priority in the allocation of resources. Highest priority will normally be given to activities considered essential to mission accomplishment.

(2) Determine if any area is overprotected, e.g., when there is a need which no longer exists and protective resources are no longer required. Practical cost-effective security measures should be the primary consideration.

(3) Establish a physical security plan.

d. Survey Report.

(1) DOT Form 1610.1, Physical Security Survey, (or appropriate FAA or USCG form) will be used for conducting physical security surveys. The

following exhibits may be attached to the survey report:

(a) Samples of personnel, visitor, and vehicular identification;

(b) Photographs and sketches clarifying elements of the report; as a minimum, a sketch/engineer drawing of the facility or office will be included;

(c) Security lists showing the priority in allocation of security resources, and a list of facilities or offices exempt from inspection; and

(d) Additional material deemed essential to support comments and recommendations. Exhibits will be identified alphabetically and in the order in which they are referred to in the narrative. An index of exhibits will be attached on a separate sheet of paper following the body of the report.

(2) Findings of the survey will be discussed at the exit interview, and a copy of the survey report will be forwarded through appropriate channels to the Facility or Office Manager within 30 days following completion of the survey.

FOR THE SECRETARY OF TRANSPORTATION:

Melissa J. Allen
For the Assistant Secretary
for Administration

SAMPLE PHYSICAL SECURITY PLAN

(Classification)

(Address of Activity/Installation)

(Copy Number)

(Issuing Operating Administration)

(Date of Issue)

PHYSICAL SECURITY PLAN

1. Purpose. State the purpose of the plan.

2. Area Security. Define the areas, buildings, etc., considered critical and establish priorities for their protection.

3. Control Measures. Define and establish restrictions on access and movement into critical areas. These restrictions can be categorized as to personnel, vehicles, and material.

   a. Personnel access:

      (1) establish access criteria and controls (regular duty hours and nonduty hours); and

      (2) identification and control systems (badges, passes, and security clearance).

b. Material control:

(1) incoming material-inspections, searches, and admission;

(2) outgoing control-documents required, inspections, etc.; and

(3) special materials-procedures for arms, ammunition, and explosives.

c. Vehicle control:

(1) policy on search of vehicles;

(2) parking regulations;

(3) controls for entrance and exit-emergency vehicles, official vehicles, and privately owned vehicles; and

(4) vehicle registration,

4. Aids to Security. Indicate the manner in which the following listed aids to security will be used.

a. Protective barriers.

b. Protective lighting.

c. Intrusion detection systems;

d. Automated entry control systems.

e. Closed circuit television systems.

f. Security communications systems Frequency Modulation (FM), Ultra High Frequency (UHF), and Very High-Frequency (VHF), telephone, etc.

5. Security Forces. Include general instructions that would apply to all security force personnel (fixed and mobile). Detailed instructions such as special orders and standard operating procedures should be attached.

a. Composition and organization.

b. Tours of duty.

c. Essential posts and routes of patrol.

d. Weapons and equipment training.

e. Alert/emergency response forces.

6. Contingency Plans. Indicate required actions in response to various emergency situations. Detailed plans such as counterterrorism, bomb threats, hostage situations, disasters, fires, etc., should be attached as annexes.

7. Coordinating Instructions. Indicate matters which require coordination with other Federal, State, and local agencies.

a. Integration of plans of -host or nearby Federal Government installations.

b. Liaison and coordination with Federal, State, and local public safety and law enforcement agencies.

_____

(Signature of Facility/Office Director or Manager)

Annexes:

a. Activity/installation security status map.

b. Contingency plans.

c. Special instructions to security officers/representatives/watch officers.

d. Security force relief instructions.

e. Sergeant of the guard instructions.

f. Special orders for guard posts.

EXAMPLES OF ACTIVITIES WHICH MAY BE CONSIDERED MISSION-ESSENTIAL/VULNERABLE AREAS

Arms, Ammunition, and Explosive Storage Areas
Airfields and Aircraft Parking/Maintenance Areas
Banking Institutions (including Credit Unions)
Bulk Material Storage Areas
Classified Storage Areas, Sites, and Locations
Cold Storage Facilities
Operations Centers
Communications Centers and Facilities
Computer Media Storage Rooms
Controlled Drug/Narcotic Vaults and Storage Areas
Data Processing/Computer Centers and Alternate Sites
Finance and Accounting Offices
Intrusion Detection System Monitoring Stations
Laboratories
Mail Rooms
Medical Supply and Storage Facilities
Motor Pools
Museums
Mew Construction Projects
OST Personnel Records Room
Pharmacies
Petroleum, Oil, and Lubricants Storage and Dispensing Points
Power Plants and Power Supply Transmission Facilities
Research and Development Activities
Supply and Equipment Pools
Shipping and Receiving Terminals
Telephone Switchboards and Switching Facilities
Utilization and Storage Section
Vessel Anchorage, Docking, and Port Facilities
Water Sources

COGNIZANT SECURITY OFFICES

OPERATING ELEMENT	COGNIZANT SECURITY OFFICE
Office of the Secretary	Office of Security (M-70)
U.S. Coast Guard	Office of Law Enforcement and Defense Operations (G-O)
Federal Aviation Administration	Office of Civil Aviation Security (ACS-1)
Federal Highway Administration	Office of Security (M-70)
Federal Railroad Administration	Office of Security (M-70)
National Highway Traffic Safety Administration	Office of Security (M-70)
Urban Mass Transportation Administration	Office of Security (M-70)
St. Lawrence Seaway Development Corporation	Office of Security (M-70)
Maritime Administration	Office of Security (M-70)
Research and Special Programs Administration	Office of Security (M-70)